View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by AUT Scholarly Commons

Security and Privacy Issues Related to the Use of Mobile Health Apps

Rajindra Adhikari and Deborah Richards

Department of Computing
Macquarie University
NSW, Australia
Email: deborah.richards@mq.edu.au

Karen Scott

The Children's Hospital at Westmead
University of Sydney
NSW, Australia
Email: karen.scott@health.nsw.gov.au

Abstract

Mobile Health applications (mHealth apps) have become integrated into the field of consumer health informatics as tools that maintain a patient-centered model of health care by allowing consumers to monitor their health related problems, understand specific medical conditions and attain personal fitness goals. However, mHealth apps may comprise significant risks to the privacy and security of consumer's protected health information. The aim of this project is to investigate the strengths and limitations of data privacy and security in the most popular mHealth apps on the market. This project involves a systematic literature review and a comparative analysis of the 20 most popular mHealth apps to identify a set of risk and safe features that can assist consumers in the selection of mHealth apps and provide guidelines for the development of mHealth apps with appropriate security and privacy measures.

Keywords

mHealth, security, privacy, Apps.

INTRODUCTION

Mobile health applications (mHealth apps) are software programs that offer health associated facilities for mobile phones and tablets (Remedy Health Media 2014). The use of mHealth apps has exploded with the introduction of the smartphone, including Google's Android platform and Apple's iPhone (Schulke 2013). mHealth apps are available to consumers while they are at home or away from home (at work, education or in transit) (Tech-Target 2009-2014). mHealth can make health services available through mobile phones, from Telemedicine, which helps health care providers monitor their patients' health conditions remotely, to basic health information services, such as getting an SMS with information about medical conditions (Technologies 2014). mHealth can also provide personalized medicine. Consumers may use mHealth apps for self-monitoring by measuring and collecting personal data such as food intake, exercise and blood sugar levels (UCSF 2012).

mHealth apps have been integrated into the field of health care in an attempt to address a wide variety of issues. mHealth apps can improve patients' health state by enabling physicians to regularly keep track of their patients' condition and connect to people in different location, while reducing costs of visits (Brookings 2013) (Care 2014). mHealth apps can also significantly improve the availability, helpfulness and affordability of healthcare for patients and reduce physical and scheduling difficulties between patients and healthcare specialists (Mirza et al. 2008).

Despite these promised benefits, there are some limitations. Many consumers do not have smartphones or do not fully understand how to use their smartphones and may be unable to use an app even if one is recommended to them (LLC 1994 - 2014). Incorrect medical advice provided by mHealth apps can be harmful as consumers may rely on the apps to treat a condition or delay seeking necessary care (Schulke 2013). mHealth apps that provide false clinical measurements can lead to unnecessary care for consumers because they may think they are sicker than they actually are.

Additionally, mHealth may pose significant risks to the privacy and security of consumers' protected health information. Sensitive data gathered by mobile health apps may be accessible to the patient, physicians, family members or scientific researchers but may also be shared with third parties, such as advertisers (Group 2013),

putting the confidentiality of consumers' information at risk. Given the increasing use of electronic health records (EHR) and electronic healthcare (eHealth), the confidentiality, integrity and availability of consumer data are today's major issues for health service providers in terms of security and data privacy (Wang et al. 2013). The research scope for this project focuses on the data privacy and security issues associated with consumer use of mHealth apps. The research questions are:

1. What are the issues related to data privacy and security involved in using mHealth apps?
2. What data privacy and security measures can be used in mHealth apps?
3. What is the risk or safety status of current mHealth apps?
4. What recommendations can be made to improve the privacy and security of mHealth apps?

To identify the data privacy and security issues (Question 1) and measures in use (Question 2) we conducted a review of the literature. To understand whether current mHealth apps adhere to the measure or pose a risk (Question 3), we analysed the 20 most popular health apps from Apple and Google stores, further described in our approach. After presenting our findings, we provide recommendations (Question 4) for consumers and developers and our conclusion.

LITERATURE REVIEW

While appropriate utilization of mHealth apps would potentially improve the quality and affordability of health care and allow patients to safely and securely connect with their physicians, Schulke (Schulke 2013) warns that the increase of free and paid mHealth apps on the market might pose health risks to patients due to a lack of health professional involvement in the development of the apps. Schulke (Schulke 2013) defines two broad classes of mHealth apps: provider-focused and patient-focused. This literature review consider data privacy and security risks of mHealth apps from a consumer perspective, covering the data of user whether a provider or patient. We present below a number of security and privacy mHealth app themes identified from the literature including: security and privacy challenge, poorly protected consumer data, data security breaches, lack of app standards/guidelines and mhealth cloud storage. Finally, we present suggested mobile devices security measures to minimise these risks.

Security and Privacy Challenges

Faudree and Ford (Faudree and Ford 2013) declared the use mHealth apps among healthcare providers and consumers may bring significant issues, such as security and privacy challenges. If healthcare providers are unable to provide adequate safeguards to patient privacy, the consequences can be significant. As evidence of the security and privacy challenges, the authors reported that a small survey found 93% of clinicians use smartphones to access EMR but only 38% follow a formal mobile privacy policy.

Data security and privacy are major concerns for personal health records according to Kharrazi, Chisholm, VanNasdale and Thompson (Kharrazi et al. 2012). The lack of standardization and security issues involved with mHealth apps are a huge barrier to their widespread use. In particular, the authors focused on the limitation of information security on a mobile device. Consumers may lose their devices or may not use any security authentication to protect the data. It is therefore the consumer's responsibility to secure their own information with device passwords and application passwords to protect their private information in the apps. The authors also emphasized that to reduce the security risks of mHealth apps, a thorough verification process is required by the app stores that could detect wicked programs.

Kane (Group 2013) stated that some mHealth apps involve an internet-enabled mobile device connecting wirelessly to portable or embedded sensors that track or measure a patient's health condition or a consumer's activities. The tracking of the patient's health perhaps occurs in real-time, with or without the patient's involvement or approval at each instant. The author focused on the data gathered by mHealth apps that access the patient and are simultaneously shared with others. The data gathered by such mHealth apps not only carry detailed information about a person's health, but also about their habits, location and movements, which possibly puts the person's sensitive information at risk if such information is disclosed.

Poorly protected Consumer data

McCarthy (McCarthy 2013) highlighted a major concern in relation to consumer data, which is generally poorly protected in mHealth apps. She reported that in a study of 43 health and fitness apps, only 74% of the free apps and 60% of the paid apps had a privacy policy, available either in the app or on the developer's website. However, only 25% of the free apps and 48% of the paid apps informed consumers about the privacy policy. Furthermore, none of the free apps and only a few of the paid apps encrypted the data that consumers entered

into the apps. Encryption is the conversion of data into a form that cannot be easily understood by unauthorized people. Therefore mHealth apps that do not encrypt consumers' information can pose a threat to data privacy.

Nasiri (HealthCareBusinessTech 2014) also reported data privacy risks in mHealth apps. He found many consumers use mHealth apps to interact with their healthcare providers, as well as track and manage symptoms and other information. Nasiri found the information consumers shared with others may carry privacy risks. He reported that researchers carried out a survey of 20 of the 23 most popular free mHealth apps and found that 50% send data to third-party advertisers and 39% send data to unidentified parties without any data encryption. He stated that paid apps are safer compared to free mHealth apps to a certain degree. Many free mHealth apps for mobile phones send data, connect to third-party sites, use unencrypted connections, allow for data collection by third parties and store data externally. Most of the time this happened without notifying users.

Data Security Breaches

Data security breaches in healthcare have become common according to Figg and Kam (Figg and Kam 2011), with many on-line mHealth providers, including doctors and scientific researchers, able to view patients' medical records without patients' knowledge. The authors also stated that the data security breaches in healthcare are a privacy threat that might lead to medical identity theft. The World Privacy Forum describe medical identity theft as an occurrence in which a person uses another person's identity, such as a person's name or Medicare number, without the person's knowledge and consent, which would impact many consumers' security (Dixon 2006). According to the US Federal Trade Commission (FTC) there were nearly 18,000 cases of medical identity theft between 2005 between 2011. Medical identity theft could result in some unauthorized benefits to the offender. The offender may steal patients' records to sell on the black market, or they may alter patients' records for fun e.g., add false entries regarding diagnosis, blood types, drug allergies and other health information. Victims who have their medical records altered by offenders may receive false medical treatment that may cause disastrous consequences to their health, possibly resulting in fatalities.

Lack of App Standards/Guidelines

Security concerns about mHealth apps are increasing due to the lack of standard app development guidelines (Kharrazi et al. 2012). Mobile payment that directly debits health service accounts or bills payer also puts consumers' security at great risks. A common occurrence such as the loss or theft of a mobile device with unencrypted consumer data, including credit card numbers, could result in a security breach with wide-ranging consequences. Fraud and identity theft caused from security breaks could also lead to mistrust among consumers and healthcare providers. However a secure mHealth environment that builds trust among consumers and healthcare service providers would need to adopt standard guidelines to increase security and protect from any unauthorized attacks (Faudree and Ford 2013).

mHealth Cloud Storage

However, mobile cloud computing brings a set of new challenges, especially when it comes to the availability of services and the security and privacy of consumers (Gu and Guirguis 2014). Security issues are critical when a healthcare provider plans to deploy a cloud-based EHR management system because moving patient data to the cloud means that patient files are hosted on the servers of the cloud service provider (Piette et al. 2011). According to Zhang and Liu (Rui and Ling 2010), when moving patient data to the cloud, healthcare providers are exposing information to several external threats because the data is available via the Internet. Both cloud service providers and healthcare providers must understand the consequences in relation to the privacy risks of consumers' sensitive data: the healthcare provider must guarantee the security of patient data by ensuring that the cloud platform has the needed security mechanisms in place (Research 2013) and it is the cloud provider's responsibility to protect the security and privacy of the information by providing the security needed to avoid external attacks to steal or even delete the information. Lack of privacy of user data and lack of regulation and guidelines for the development of mHealth apps need to be considered for the improvement of mHealth apps.

Mobile Devices Security Measures

Mobile technology is the technology used for cellular communication. The US Office of Civil Rights (OCR) recently launched an educational initiative for mobile devices (HealthIt 2014), which identified the following guidelines for app developers: Know the risks; Take the steps; Protect and secure health information. Table 1 summarises measures suggested by OCR (HealthIt 2014) (Senft 2013) to ensure that mHealth information is secure when using mobile devices such as smartphones and tablets. The OCR reported that a significant number of data privacy breaches each year arise from lost or stolen mobile devices.

Table 1. Measures to ensure mHealth information is secure (HealthIt 2014) (Senft 2013)

Measure	Description
Use of a password or other user authentication	Mobile devices can be configured to require passwords, personal identification numbers (PINs), or passcodes to gain access. The password, PIN, or passcode field can be masked to prevent people from seeing it
Install & enable encryption on mobile devices	Encryption renders data unusable, unreadable, and undecipherable to unauthorized individuals.
Activate remote wiping and/or remote disabling	Remote wiping allows an individual to permanently erase all data stored on a mobile device remotely, such as when the device is stolen. With remote disabling, if the mobile device is later recovered, unlock can re-access data.
File-sharing applications or software	File sharing is designed to allow Internet users to connect and share or trade files. Enabled file sharing could provide unauthorized users with access to a mobile device without user knowledge.
Firewall	A personal firewall can protect against unauthorized connections by intercepting incoming and outgoing connection attempts and blocking or permitting the connection based on an established predetermined set of rules
Security software	Security software can be installed and regularly updated to protect against malicious applications, viruses, spyware, and malware-based attacks. Be wary of malicious software in email attachments, websites or downloaded programs.
Using non-secured Wi-Fi network or hotspot	Without using a secured Wi-Fi network, there is a risk that communications will be intercepted. Users should avoid sending or receiving information when connected to a public wireless Internet.
Delete mHealth information	Delete or wipe all data stored on a mobile device before discarding the device. Use software to overwrite the data, or devices that purge or destroy the data.

METHODOLOGY

To determine to what extent current mHealth apps pose a data privacy and security threat and, where necessary, recommend solutions, we have chosen to conduct a comparative analysis as a case study of the twenty most popular free and paid mHealth apps from Apple and Google stores. The process involved the following three steps.

1. Selection criteria for 20 mHealth apps
2. Identification of data privacy and security features and issues of mHealth apps
3. Comparative analysis of 20 mHealth apps

The selection of the apps was determined by: highest number of downloads on the mHealth market, with high ratings from consumers, search engines or mobile app stores; and recommended by social media.

Privacy issues related to using mHealth apps include a breach of consumer confidentiality, data privacy shortcomings, security problems and lack of health professional participation in the development of apps. To accelerate adoption of mHealth it is important to put in place supportive privacy policies (P A Consulting 2012). A clear privacy policy can tell consumers what permissions an app requires of the device before downloading it such as geo-location services access, book access, camera access, phone call access and contacts access. Therefore if consumers are not comfortable with mHealth apps that are asking many permissions, they should avoid downloading them. From the literature we identified a set of eight features that we categorised as security risks (first three) or safety measures (last five). We ask the following questions to measure each app against these features we ask the questions.

Does the app ask for user registration (name, address, birthday and email)? Most mHealth apps available on the market ask for consumers' details prior to register the apps. It is consumers' responsibility whether or not to provide information to those mHealth apps. Providing detailed information may result in compromising data privacy.

Are consumers able to update and correct their personal profiles? This allows consumers to change their individual profiles according to the policy of the mHealth apps. Updating patient records improves data accuracy and supports better patient care.

Does an app ask for user authentication (user name and password)? Some of the most common threats to data security and patient privacy come from unauthorized access. The purpose of the security evaluation is to check security mechanisms (username and password) are implemented to guarantee the privacy of consumers' data.

Can consumers delete any personal information completely? It is a prime concern whether mHealth apps allow consumers to delete their personnel information completely. When consumers stop using a mHealth app, they need to be able to delete it. They also need to be able to delete their personal profile and any data archives that have been created with their personal information.

Where is data stored (locally on a device or in a cloud)? Data storage is the recording and storing of consumer information. Data storage can either be possible locally on the mobile device or in cloud storage, depending upon the development of the mHealth app.

Is consumer data shared with a third party or advertiser? Sharing of mHealth consumer data with a third party or advertiser is becoming a more serious concern as many mobile apps share consumers' data to generate revenue or cost. mHealth apps collect detailed personal and health information from consumers to provide better services for health and well-being, but sharing sensitive health information with third parties and advertisers impacts many consumers' data privacy and security.

Are consumers informed about any data privacy and security measures? Ensuring the privacy and security of health information, including information in electronic health records (EHR), is a key component to building the trust required to realize the potential benefits of electronic health information exchange. Healthcare providers are working to design and implement security and privacy measures to support the deployment of mHealth apps.

Is there a privacy policy? The privacy policy sets out how a mHealth app uses and protects any information that consumers give to app owners when using the mHealth app.

RESULTS OF SELECTION PROCESS OF 20 APPS

In this section we present the evaluation results of the 20 most used mHealth apps on the market. The results are based on the privacy and security features of the mHealth apps. To conduct the comparative analysis, all 20 apps were downloaded onto a corresponding device (iPhone or Android smartphone). We analysed the app's authentication functions and features relating to consumer data privacy (relating to the first eighth comparative analysis criteria), as well as the privacy policy on the developers' websites (the ninth comparative analysis criteria). A description of each app and how it met the selection criteria is provided below. Summary results to the comparison questions can be found in Table 3.

Apple Stores

MyFitnessPal (MyFitnessPal 2005 - 2014) is an online and app-based wellness-tracking platform. It is a calorie counter and exercise tracker. It helps to evaluate how many calories the user has eaten versus how many they have burnt. The app can also help to track over time any changes, such as weight or waist size. It provides the services for informational purposes only. No medical professionals were involved in its development.

Medscape (Medscape 1994 - 2014) mobile, developed by WebMD, is the leading medical resource mostly used by physicians, medical students, nurses and other health care professionals for clinical information. It supports clinicians with all of their professional needs, including decision-making at the point-of-care, medical news and professional development. This is the highest rating and fastest growing free mHealth app with over 4 million registered users.

Epocrates (Epocrates 2014) is the most popular mHealth app among U.S physicians for clinical content and decision support at the point of care. Epocrates has a reliable link of more than a million health care professionals and is used to find providers, review drug prescribing and safety information for thousands of brand and generic medications and identify pills by imprint code and physical characteristics. The app, built by Epocrates, got 2nd place out of 15 apps reviewed by iMedicalApps Team (iMedicalApps Team 2011).

NeuroMind (DigitalNeurosurgeon 2014) offers interactive clinical decision support. It contains more than 120 clinical classification and grading systems, and some anatomical images for explanation to patients and students. This application has been developed with the involvement of Surgical Neurology International, the European Association of Neurosurgical Societies (EANS), and Neurosurgic.com and considered the number one app for neurosurgery in the world, with over 200,000 downloads.

Smart Blood Pressure (SmartBP) (Systems 2012) is an easy-to-use blood pressure management tool that helps patients manage and take control of their health using their mobile device. SmartBP allows users to record, analyze and share blood pressure information. This application has been developed with the involvement of Evolve Medical Systems. SmartBP tracks progress and manages all blood pressure measurements with an overall goal of improving blood pressure. Blood pressure, pulsing rate and weight can be shared with anyone using email and text message.

Pill Monitor (Appato 2012) is designed to manage and remind users to take pills on time. Taking pills on time and at the same time every day is good for health. This app is very simple and easy to use. The app was built by Maxwell software and got 4 stars out of 5 based on 353 ratings and 53 user reviews. Key features are schedule

reminder of pill, consumer reminder time, repeat date and dosage of pills, check current reminders and upcoming reminders and allow users to add photos to each pill.

Pregnancy & Baby app (Inc. 2014) is designed to look at pregnancy phases. Based on the baby's due date, consumers can receive personalized content and get access to the latest parenting news and health information. It also includes a short video of common symptoms and recommendations and helps consumers to access a variety of online communities. The app was built by Everyday Health Inc. and got 4 stars out of 5 based on 3330 votes.

Diabetes Tracker Plus (Apptism 2013) helps people with diabetes to control blood glucose and stay in good health. Logging and tracking blood sugar using the app supports consumers to self-manage and self-track diabetes. Blood sugar logs and reports can be shared with a healthcare provider by emails. There is no information about health professional involvement in the development of the app. This app is recommended by MyNetDiary Diabetes (Inc 2013).

Growth app (Apps 2014) helps to track the growth curves of newborn babies as well as older children and compare progress with expected growth rates. This app helps consumers to share the results with family, friends or health professionals. The development of the app did not involve any health professionals. Growth charts are designed in accordance with and recommended by World Health Organization (WHO) and Centre for Disease Control.

Instant Heart Rate (Azumio 2012) uses iPhones' camera to detect pulse from the fingertip. Prior using the Instant heart rate app, consumers need to place the tip of their finger on the camera for few seconds. A real time chart will show every heartbeat. This app has received the best Health and Fitness app on Mobile Premier Awards 2011. Azumio Inc. was involved in the development of the app and more than 25 million users already using it. There was no any health professional involvement for the development of the app.

Google Store Apps

Ob (Pregnancy) Wheel app (Play 2014d) is a free android pregnancy calculator. Many clinicians find this app useful, such as those working in primary care, emergency departments and obstetrics. Numerous adjustable preferences and settings, ultrasound exam dating, and dating ordered patient lists make Ob (Pregnancy) Wheel the best among several free and paid OB wheels on the Android Market (iMedicalApps Team 2011). Though developed without professional input, this app is recommended by iMedicalApps Team (iMedicalApps Team 2011) and has got 4.2 stars out of 5 based on 1208 user reviews.

Calorie Counter (Play 2014a) is the app to simply find nutritional information for the food that users eat and easily keep track of meals, and counseling patients about diet, exercise and weight. Users are able to look up almost any type of food category; fast foods, grocery store food, and prepared foods. Consumers can even scan barcodes with a camera and the app identifies the type of food along with allocating the appropriate calories. The app was built by MyFitnessPal, Inc and has got 4.7 stars out of 5 based on 618,588 user reviews.

The skyscape medical resources app (Play 2014f) is a decision support tool that helps physicians, nurses and students to find the right answers of medical resources such as medical calculators, periodically updated medical news alerts, select practice guidelines and disease monographs. More than 2.7 million healthcare professionals access the medical resources in this app. This app is recommended by iMedicalApps Team (2011).

Endomondo app (Play 2014b) helps to track consumers' workouts and analyze their training. This app can be used as a free personal trainer and social fitness partner. This app is used for running, cycling and walking and is one of the highest rated apps on Android market. Though it was developed with health professional input, more than 20 million users are taking advantage of Endomondo app and has got 4.5 stars out of 5 based 166,459 user reviews.

iTriage app (iTriage 2013) is a consumer healthcare company founded in 2008 by two emergency medicine physicians. Over 7 million users have downloaded iTriage app and used it to locate nearby providers based on their symptoms, make appointments, store their personal health record, save medication refill reminders, and learn about medications, diseases and procedures. iTriage aims to help answer questions such as: "What medical condition could I have?" and "Where should I go for treatment?

Appointuit app (Appointuit 2012) helps consumers make an appointment with doctors anywhere, anytime. This app can also cancel and reschedule an appointment if needed. Android apps market recommended this app.

Cardiograph app (Ltd 2011 - 2013) is used to measure users' heart rate. The app can save results for future reference and keep track of multiple people with individual profiles. It uses a mobile device's built-in camera to take pictures of a user's fingertip and calculate their heart's rhythm. The app was built by MacroPinch and has got 4 stars out of 5 based on 61,195 user reviews.

Quit now app (Play 2014e) offers a real-time stats anytime to help users quit smoking. The indicators tell users how long it has been since they last smoked and the money the user saved. It also shows various indicators for how much the user's heath has improved since they stopped smoking. The app was built by Fewlaps and has got 4 stars out of 5 based on 9,780 user reviews.

GI Monitor (Play 2014c) is a symptom logging application for patients with IBD (Inflammatory Bowel Disease), Crohn's or Ulcerative Colitis. This app allows patients to easily and accurately log symptoms and provide data to their doctors for optimal treatment. There is not any healthcare personal involved in the development of the app. This app is recommended by WellApps, medivo (WellApps 2009 - 2011).

Stress Check (Play 2014g) is an app available for quantifying the level of psychological or physical stress. By measuring patient heart rate through the camera and light features on smartphones, Stress Check can estimate the level of stress in real time. The app was built by Azumin Inc. and got 3.5/5 stars based on 4,223 user reviews.

RESULTS: COMPARATIVE ANALYSIS

Table 2 shows a summary of the comparison analysis of 20 mHealth apps. The results illustrate that not all mHealth apps available in the app stores are free of issues. Out of 20 apps only one app enables consumers to delete personal information completely and only 5% or 1 of the apps mentioned that users can delete their personal information completely. According to the study 65% or 13 of the apps asked consumers to enter personal information such as name, address, email and DOB but only two apps asked for consumers' authentication prior to log-in to the apps. Half (50% or 10 apps) stored data in a cloud that significantly pose risks of consumers' data privacy and 65% or 13 of the apps shared consumers' information to a third party or advertisers. Few apps (20% or 4) informed consumers about data privacy and security measures, however, 90% or 18 of the apps have a privacy policy that explains the details of the apps' privacy and security measures.

Table 2. mHealth App Comparison Results

	* registration	* cloud storage	* third party	authentication	update profiles	complete delete	local data	security explained	privacy policy	*risk score (3)	safe score (6)
Myfitnesspal	1	1	1	-	1	1	-	-	1	**3**	**3**
Medscape	1	1	-	1	1	-	-	1	1	**2**	**4**
Epocrates	1	1	1	-	-	-	1	-	1	**3**	**2**
Neuromind	-	-	-	-	-	-	1	-	1	**0**	**2**
Smart Bp	-	-	-	-	-	-	1	-	1	**0**	**2**
Pill Monitor	-	-	1	-	-	-	1	-	-	**1**	**1**
Pregnancy & Baby	1	1	1	1	-	-	1	-	1	**3**	**3**
Diabetes Tracker Plus	1	-	-	-	1	-	1	-	1	**1**	**3**
Growth	1	-	-	-	1	-	1	-	1	**1**	**3**
Instant Heart Rate	1	-	1	-	-	-	1	-	1	**2**	**2**
Ob (Pregnancy)	-	-	1	-	-	-	1	-	-	**1**	**1**
Calorie Counter	1	1	1	-	-	-	-	-	1	**3**	**1**
Skyscape	1	1	1	-	1	-	1	1	1	**3**	**4**
Endomondo	1	1	1	-	-	-	-	-	1	**3**	**1**
Itriage	1	1	1	-	1	-	-	1	1	**3**	**3**
Appointuit	1	1	1	-	1	-	-	1	1	**3**	**3**
Cardiograph	-	-	-	-	-	-	1	-	1	**0**	**2**
Quit Now	-	-	1	-	-	-	1	-	1	**1**	**2**
Gi Monitor	1	1	1	-	1	-	1	-	1	**3**	**3**
Stress Check	-	-	-	-	-	-	1	-	1	**0**	**2**
Total	**13**	**10**	**13**	**2**	**8**	**1**	**14**	**4**	**18**		

Even though apps such as "Medscape" and "Skyscape" have higher safe score of 4 out of 6 but apps have also considerably higher risk score, which makes those apps as per my analysis, is risk to use. As shown in Table 2 some apps such as "Diabetes Tracker Plus" and "Growth" ask users personal information. Apps such as "Quit Now", "Pill Monitor" and "Ob Pregnancy" have risk score 1 out of 3 but these apps are low risk to use as none of these apps ask user personal information. "NeuroMind", "Smart BP" "Cardiograph" and "Stress Check" apps were found to be relatively safe to use compared to other apps. These apps do not ask for personal user details prior to log-in to the apps. Furthermore, they allow consumers to store results locally on the mobile device and do not share consumer data with a third party or advertisers. Even though none of the apps ask consumers for authentication, such as user name and password, to log-in to the app, theses apps are safe to use as they do not require consumers to enter personal information.

In this mHealth app evaluation only 20% of the 20 apps implement security measures to ensure privacy and security of consumers' information. These involve the use of firewalls, secure connections on the websites, frequently the use of secured socket levels (SSL) that encrypt pages that collect user information and the security methods such as authentication to determine the identify of registered users, so that appropriate rights and restrictions can be enforced for that user. The lack of security measures and data privacy has previously been noted by my researchers by McCarthy (2013), who underlined that in a study of 43 health and fitness apps, only a few of the paid apps encrypted the data that consumers entered into the apps.

McCarthy (2013) also reported that the consumer information entered into apps is poorly protected without any authentication and security mechanisms. Out of 43 health and fitness apps he examined, 74% of free and 60% of paid apps had a privacy policy in the app or on the developer website. According to our analysis of 17 free and three paid mHealth apps, we found that 88% of free mHealth apps and 100% of paid mHealth apps have a privacy policy. But only 23% free apps and 0% paid apps informed consumers about security measures. Nasiri (HealthCareBusinessTech 2014) surveyed of 20 of the 23 free mHealth apps and found that 50% transfer information to third party and 39% send data to unidentified parties without consumer consent. We found that 65% of the reviewed apps send consumer data to a third party or advertisers.

In brief, the main risks posed to data protection by apps are the consumers' lack of knowledge about the app, insufficient security measures to safeguard consumers' sensitive data, information shared with third party or advertisers and lack of user authentication prior to log-in to the app such as user name and password. Therefore we recommend that apps should only collect data that is strictly necessary for the app to perform the desired functionality. A set of recommendations to consumers and application developers can be found in Table 3.

Table 3. Recommendations to Consumers and Application Developers

Consumers	Application developers
Research the app before downloading it	Sensitive consumers' information should always be stored encrypted so that attackers cannot simply retrieve this data off of the file system.
Try to use apps without entering personal information if permitted	Apps should be designed to help patients through the evolution of a disease and provide recommendations
Look for user reviews and the privacy policy of an app, either through the app store or online.	Include user authentication. Provide options so user can safely retrieve their login details if forgotten. Only 10% or 2 apps out of 20 apps ask for user authentication prior to log-in.
Remove data when usage stopped. This may prevent unauthorised use of stored data when consumers no longer use the apps.	Minimise sharing information with third parties or advertisers and ask users to confirm agreement before sharing. 65% or 13 apps shared consumers' information to third parties or advertisers.
Give feedback on product: Users' feedback on the features, privacy and policy, and functions of an app will help the developers to restructure the app appropriately.	Apps should allow consumers' to delete their personal information completely. According to the analysis only 5% or 1 apps mentioned in its privacy policy that consumers can delete information completely therefore this criteria need to be improved appropriately.
	Provide user with information about the implementation of security measures and authentication and what how/where their data is stored.

CONCLUSION

This comparative analysis of 20 mHealth apps illustrated that not all mHealth apps available in the app stores are free of privacy and security issues. Major areas that need to be focussed on in order to develop secure apps are standard app development guidelines and security authentication measures, such as device and app passwords, appropriate encryption mechanisms and an informative privacy policy on each app. As future work, it would be important to analyse the security mechanisms and encryption methods of the apps. As it is unlikely that the vendor will provide this information, discovery of these methods would probably involve trying to hack into the app, a dubious activity that we did not want to undertake. The study seeks to prepare consumers, healthcare personal and app developers to take caution when adopting and developing mHealth apps by providing them with the knowledge about app issues as well as benefits and risk associated with mHealth apps in healthcare.

REFERENCES

Appato. 2012. "Pill Monitor Free- Medication Reminders and Logs." Retrieved 07 - May - 2014, from http://www.appato.com/maxwell-software/pill-monitor-free-medication-reminders-and-logs/#

Appointuit. 2012. "Appointuit." Retrieved 10 - May - 2014, from http://appointuit.com/why

Apps, C. 2014. "Follow Your Child's Growth." Retrieved 10 - May - 2014, from www.growthapp.net

Apptism. 2013. "Diabetes Tracker Plus Health & Fitness App." Retrieved 09 - May - 2014, from http://www.apptism.com/health-fitness/ooober-inc/diabetes-tracker-plus/

Azumio. 2012. "Instatnt Heart Rate." Retrieved 10 - May - 2014, from www.azumio.com/apps/heart-rate/

Brookings, C.f.T.I.a. 2013. "Improving Health Care through Mobile Medical Devices and Sensors." Retrieved 10 - April - 2014, from http://www.brookings.edu/~/media/research/files/papers/2013/10/22%20mobile%20medical%20devices%20west/west_mobile%20medical%20devices_v06.pdf

Care, S.H. 2014. "Health Care on the Go." Retrieved 01 - May - 2014, from http://www.supplementalhealthcare.com/blog/2013/healthcare-go-pros-and-cons-mobile-health-apps

DigitalNeurosurgeon. 2014. "Description." Retrieved 04 - May - 2014, from http://blog.digitalneurosurgeon.com/ & http://itunes.apple.com/us/app/neuromind/id353386909?mt=8

Dixon, P. 2006. "Medical Identity Theft: The Information Crime That Can Kill You," *The world privacy forum*.

Epocrates. 2014. "Epocrates, with You at the Moment of Care." Retrieved 04 - May - 2014, from www.epocrates.com

Faudree, B., and Ford, M. 2013. "Security and Privacy in Mobile Health," *CIO Journal*).

Figg, W.C., Ph.D, and Kam, H.J., M.S. 2011. "Medical Information Security," *International journal of Security (IJS)* (5:1).

Group, V. 2013. "Evaluating Mhealth Adoption Barriers: Privacy and Regulation." Retrieved 01 - April - 2014, from http://mhealthregulatorycoalition.org/wp-content/uploads/2013/01/VodafoneGlobalEnterprise-mHealth-Insights-Guide-Evaluating-mHealth-Adoption-Privacy-and-Regulation.pdf

Gu, Q., and Guirguis, M. 2014. "Secure Mobile Cloud Computing and Security Issues," in *High Performance Cloud Auditing and Applications*. Springer, pp. 65-90.

HealthCareBusinessTech. 2014. "Mobile Health Apps Create Privacy Risk, Study Says." Retrieved 18 - March - 2014, from http://www.healthcarebusinesstech.com/mobile-health-apps-privacy/

HealthIt. 2014. "Your Mobile Device and Health Information Privacy and Security." Retrieved 26 - April - 2014, from http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

iMedicalApps Team. 2011. "Top 15 Free Android Medical Apps for Healthcare Professionals." Retrieved 10 - May - 2014, from http://iims.uthscsa.edu/sites/iims/files/Top%2015%20Free%20Android%20Medical%20apps%20for%20Healthcare%20professionals.pdf

Inc, M.D. 2013. "Mynetdiary Diabetes." Retrieved 22 - May - 2014, from http://www.mynetdiary.com/diabetes-tracker-for-iPhone.html

Inc., A. 2014. "Pregnancy & Baby What to Expect." from https://itunes.apple.com/au/app/pregnancy-baby-what-to-expect/id289560144?mt=8

iTriage. 2013. "Itriage - Take Charge of Your Health." Retrieved 10 - May - 2014, from https://www.itriagehealth.com/

Kharrazi, H., Chisholm, R., VanNasdale, D., and Thompson, B. 2012. "Mobile Personal Health Records: An Evaluation of Features and Functionality," *Int.l Journal of Medical Informatics* (81:9), 9//, pp. 579-593.

LLC, W. 1994 - 2014. "Public Health in the Smartphone Era." Retrieved 15 - April - 2014, from http://www.medscape.com/viewarticle/776278_3

Ltd, M. 2011 - 2013. "Cardiograph – Personal Heart Rate Meter." Retrieved 10 - May - 2014, from http://macropinch.com/cardiograph/

McCarthy, M. 2013. "Experts Warn on Data Security in Health and Fitness Apps." p. 1.

Medscape. 1994 - 2014. "Definition." Retrieved 04 - May - 2014, from http:// www.Medscape.com/

Mirza, F., Norris, T., and Stockdale, R. 2008. "Mobile Technologies and the Holistic Management of Chronic Diseases," *Health informatics journal* (14:4), December 2008 2014-01-15, pp. 309-321.

MyFitnessPal. 2005 - 2014. "Lose Weight with Myfitnesspal." Retrieved 04 - May - 2014, from http://www.myfitnesspal.com/

P A Consulting, G. 2012. "Policy and Regulation for Innovation in Mobile Health." Retrieved 16 - April - 2014, from http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/04/policyandregulationforinnovationinmobilehealth.pdf

Piette, J.D., Mendoza-Avelares, M.O., Ganser, M., Mohamed, M., Marinec, N., and Krishnan, S. 2011. "A Preliminary Study of a Cloud-Computing Model for Chronic Illness Self-Care Support in an Underdeveloped Country," *American journal of preventive medicine* (40:6), pp. 629-632.

Play, G. 2014a. "Calorie Counter by Fat-Secret." Retrieved 08 - May - 2014, from https://play.google.com/store/apps/details?id=com.fatsecret.android

Play, G. 2014b. "Endomondo Sports Tracker." Retrieved 10 - May - 2014, from https://play.google.com/store/apps/details?id=com.skyscape.android.ui

Play, G. 2014c. "Gi Monitor." Retrieved 12 - May - 2014, from https://play.google.com/store/apps/details?id=com.wellapps.gimonitor

Play, G. 2014d. "Ob Pregnancy Wheel." Retrieved 09 - May - 2014, from https://play.google.com/store/apps/details?id=com.quartertone.medcalc.obwheel

Play, G. 2014e. "Quit Smoking- Quit Now." Retrieved 10 - May - 2014, from https://play.google.com/store/apps/details?id=com.EAGINsoftware.dejaloYa

Play, G. 2014f. "Skyscape Medical Resources." Retrieved 10 - May - 2014, from https://play.google.com/store/apps/details?id=com.skyscape.android.ui

Play, G. 2014g. "Stress Check by Azumio." Retrieved 12 - May - 2014, from https://play.google.com/store/apps/details?id=com.azumio.android.stresscheck

Remedy Health Media, L. 2014. "Health Mobile Apps Raise Concerns About Safety, Privacy, Health Costs." Retrieved 11 - April - 2014, from http://www.healthcentral.com/diet-exercise/c/255251/162564/apps-concerns-privacy/

Research, J.o.M.I. 2013. "Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems." Retrieved 03 - April - 2014, from http://www.jmir.org/2013/8/e186/

Rui, Z., and Ling, L. 2010. "Security Models and Requirements for Healthcare Application Clouds," *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, pp. 268-275.

Schulke, D.F. 2013. "The Regulatory Arms Race: Mobile-Health Applications and Agency Posturing," *Boston University Law Review* (93:5).

Senft, D.J. 2013. "Mobile Devices: Technology Aid--Security Risk," *Geriatric nursing (New York, N.Y.)* (34:2), 2013 (Epub 2013 Mar, pp. 149-150.

Systems, E.M. 2012. "Smart Blood Pressure." Retrieved 04 - May - 2014, from http://www.evolvemedsys.com/> and <https://itunes.apple.com/au/app/blood-pressuresmart-blood/id519076558?mt=8

Tech-Target. 2009-2014. "Definition: Mhealth." Retrieved 31 March 2014, from http://searchhealthit.techtarget.com/definition/mHealth>

Technologies, A. 2014. "Mhealth - Its Advantages and Disadvantages." Retrieved 16 - April - 2014, from http://attunelive.com/blog/mhealth-its-advantages-disadvantages/

UCSF. 2012. "Self-Tracking May Become Key Element of Personalized Medicine." Retrieved 01 - May - 2014, from https://www.ucsf.edu/news/2012/10/12913/self-tracking-may-become-key-element-personalized-medicine

Wang, J., Zhang, Z., Xu, K., Yin, Y., and Guo, P. 2013. "A Research on Security and Privacy Issues for Patient Related Data in Medical Organization System," *Int.l Journal of Security & Its Applications* (7:4).

WellApps. 2009 - 2011. "Well Apps." Retrieved 12 - May - 2014, from http://www.wellapps.com/

INTELLECTUAL PROPERTY

This work is licensed under a Creative Commons Attribution-NonCommercial 3.0 Australia License.
To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/3.0/au/